IN THE CLAIMS

Please amend the claims as follows:

Claims 1-2 (Canceled).

Claim 3 (Currently Amended): A terminal comprising:

an ad-hoc key management list table having at least one key management list in which authentication header keys with respect to other terminals of an ad-hoc network are held in such a manner as to correspond to the terminal identifiers of said other terminals;

means for searching said key management list for said key management list entry containing the transmission terminal identifier of a received frame in order to extract said corresponding authentication header key; and

means for confirming whether or not the authentication header of said frame is valid by using said extracted authentication header key,

a path table having at least one path list for holding a transfer destination terminal identifier for causing a frame to arrive at another terminal via terminals of the path list in such a manner as to correspond to the terminal identifier of the other terminal; and

means for searching said path table for said path list containing an end-point terminal identifier and transmitting said frame to said transfer destination terminal identifier via terminals of the path list, when said authentication header is valid and the end-point terminal identifier of said frame is not the terminal identifier of the other terminal and for discarding said frame when said authentication header is not valid,

wherein the terminal and the other terminal's communicate directly, in an ad-hoc manner, exclusive of any network access point.

Claim 4 (Cancelled).

Claim 5 (Previously Presented): A terminal comprising:

an ad-hoc key management list table having at least one key management list for holding an authentication header key and a unicast encryption key with respect to another terminal of an ad-hoc network in such a manner as to correspond to the terminal identifier of said other terminal;

means for searching said key management list table for said key management list containing the transmission terminal identifier of a received frame in order to extract said corresponding authentication header key;

means for confirming whether or not the authentication header of said frame is valid by using said extracted authentication header key;

means for searching said key management list table for said key management list entry containing a start-point terminal identifier of said frame in order to extract said corresponding unicast encryption key when said authentication header is valid and the end-point terminal identifier of said frame is the terminal identifier of the other terminal; and

means for decrypting the payload of said frame by using said extracted unicast encryption key,

wherein the terminal and the other terminal's communicate directly, in an ad-hoc manner, exclusive of any network access point.

Claim 6 (Canceled).

Claim 7 (Previously Presented): A terminal comprising:

an ad-hoc key management list table having at least one key management list for holding authentication header keys and unicast encryption keys with respect to other

terminals of an ad-hoc network in such a manner as to correspond to the terminal identifiers of said other terminals;

means for searching said key management list table for said key management list entry containing the reception terminal identifier of a frame to be transmitted in order to generate an authentication header by using said corresponding authentication header key and for giving the authentication header to said frame;

means for searching said key management list table for said key management list containing the end-point terminal identifier of said frame and for encrypting the payload of said frame by using said corresponding unicast encryption key; and

means for transmitting said frame,

wherein the terminal and the other terminal's communicate directly, in an ad-hoc manner, exclusive of any network access point.

Claims 8-12 (Canceled).

Claim 13 (Previously Presented): An encryption method for use in a terminal having an ad-hoc key management list table having at least one key management list for holding authentication header keys and unicast encryption keys with respect to other terminals of an ad-hoc network in such a manner as to correspond to the terminal identifiers of said other terminals, said encryption method, comprising:

searching said ad-hoc key management list table for said key management list entry containing the transmission terminal identifier of a received frame in order to extract said authentication header key;

confirming whether or not the authentication header of said frame is valid by using said extracted authentication header key;

searching said key management list table for said key management list containing the start-point terminal identifier of said frame when said authentication header is valid and the end-point terminal identifier of said frame is the terminal identifier of the corresponding terminal in order to extract said corresponding unicast encryption key; and

decrypting the payload of said frame by using said extracted unicast encryption key,

wherein the terminal and the other terminal's communicate directly, in an ad-hoc manner, exclusive of any network access point.

Claims 14-16 (Canceled).